Computer crime

Background Paper BP-87E

COMPUTER CRIME

Monique Hébert
Marilyn Pilon
Law and Government Division

February 1984
Revised November 1991

Library of Parliament
Bibliothèque du Parlement

Research Branch

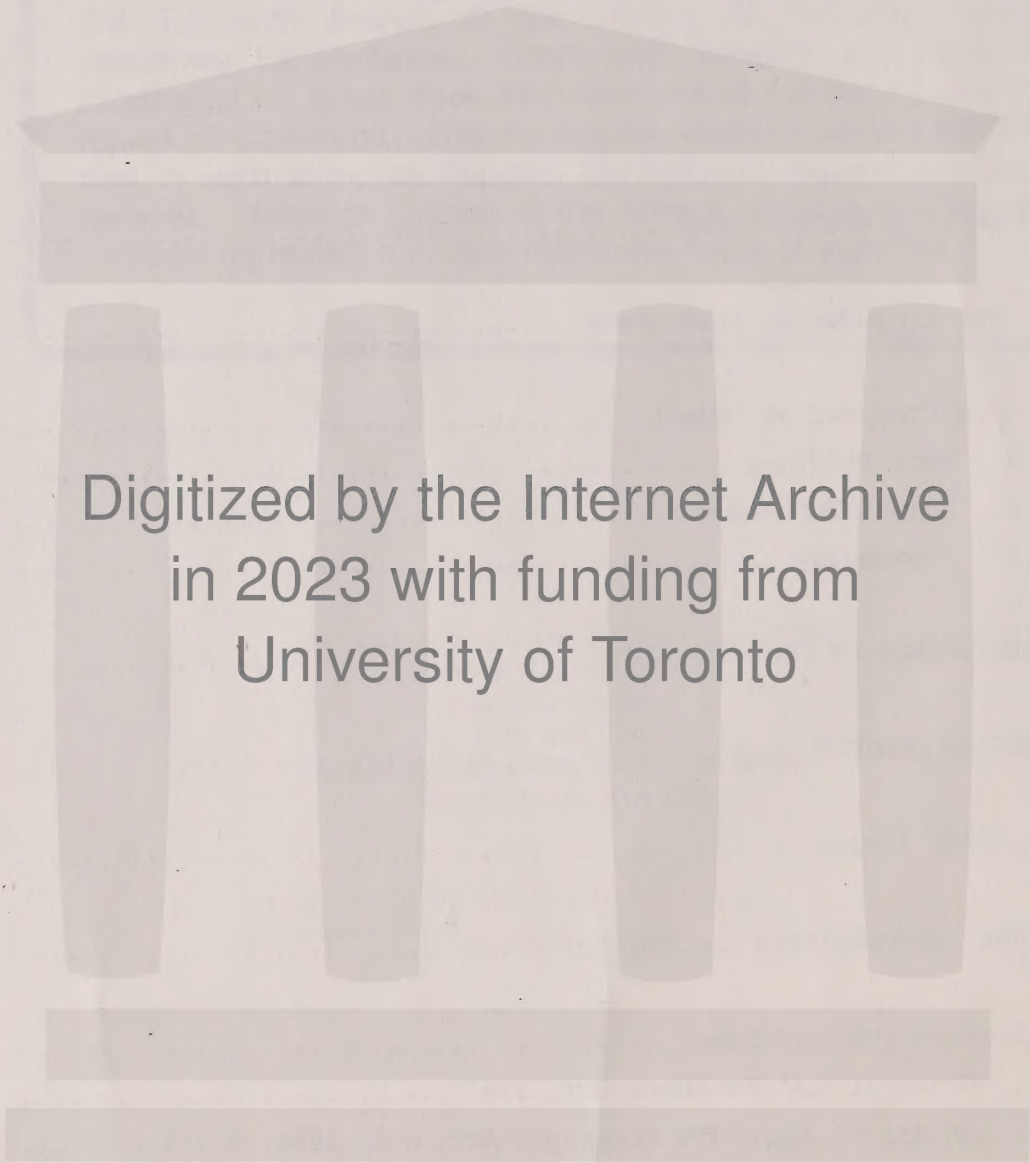
The Research Branch of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Research Officers in the Branch are also available for personal consultation in their respective fields of expertise.

Available in Canada through
your local bookseller
or by mail from
Canada Communication Group -- Publishing
Ottawa, Canada K1A OS9

Catalogue No. YM32-2/87-1991E
ISBN 0-660-14590-1

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

TABLE OF CONTENTS



COMPUTER CRIME*

INTRODUCTION

Over the past 20 years the technology of electronic data processing - the computer - has come to play a dominant role in business and government. It would be difficult to conceive of a person whose life is not in some way affected by the computer, for virtually everyone who has a bank account, engages in any kind of credit transaction, or has dealings with the government or any large organization is touched in some way by the technology. The computer is now an indispensable tool for banking, corporate records and various activities of government.(1)

But the same features of the technology that make it such a boon to society at the same time increase its susceptibility to abuse. The absence of tangible printed records of credit transactions is testimony to the efficiency of the computer, yet it leaves the auditor without the accustomed "paper trail" with which accounts can be verified. A computer need not be manipulated at any particular place, but can be operated from a distance using telecommunications facilities. This too can increase the potential for abuse, for now a thief need not be anywhere near the site of the crime but can, from the relative safety of a computer terminal, acquire assets reduced to electronic impulses.

Losses attributed to criminal activities involving the use of computer systems are a subject of some controversy. No detailed study has ever been undertaken in Canada, in part because there is no consensus as to what exactly is a "criminal activity involving the use of computer systems." In any event, it is difficult to establish with any confidence

---

* This paper is based on work done by Donald MacDonald.

(1) T. Whiteside, *Computer Caper,* Crowell and Co., New York, 1978, p. 2.

the losses from computer-crime without some clear conception of what such crime entails, and an accurate record of its frequency. Governments can have some effect on the former by defining which activities in relation to the computer are to be considered beyond acceptable standards of conduct. This may in turn have an effect on the degree to which computer abuse is reported.

DEFINITION OF COMPUTER CRIME

One very obvious question that arises in connection with the phrase "computer crime" is why should a certain area of conduct qualified by the adjective "computer" be fenced off for special consideration. We do not study filing cabinet crime, auto crime or television crime. Why should the instrument of the act make any difference? Is not theft still theft whether perpetrated with the use of break and enter tools or with a computer terminal?(2)

One response to this position is that the law is not only concerned with the prohibited ends of conduct, but also with the means used to attain those ends.

> The advent of the computer did not create a new crime, any more than the development of the automobile created a new form of larceny. As with the automobile, the criminal use of computer technology has increased the vulnerability of the community, and to the extent that the definition of crimes and the enactment of prohibitions is directed to the protection of the community, computer technology is a legitimate area of penal concern.(3)

Laws not only must enable the redress of wrongs or the punishment of the wrongdoer; they must also proscribe conduct; the complexity of the means for misconduct afforded by computer technology merits its special treatment.

---

(2) J. Becker, *The Investigation of Computer Crime*, U.S. Department of Justice, Washington, 1980, p. 1.

(3) D. Ingraham, "On Charging Computer Crime" (1980), 2 *Computer Law Journal*, 429.

Thus, as the criminal law has been modified in some respects to take account of the automobile, so also will the computer engender changes. But beyond this, even more fundamental issues arise. A distinction must be made here between types of computer crime or abuse, between the computer as the "instrument" of crime and as the "object" of crime:

A. The Computer as Instrument

In these situations the computer is used as a means to an end. Here the criminal feeds false data into a computer in order to inflate the value of a cheque; or fiddles with an accounting program to cover up embezzlement; or forges bank deposit slips to gain an illicit windfall from customers who unknowingly use them to deposit money to the crimnal's account. In each case the thief uses the computer as the instrument of the crime. The means are novel, but the intent and the object are common - to acquire someone else's money without being entitled to it.

B. The Computer as Object

Where the computer is the instrument of crime we have familiar landmarks with which to identify the conduct as criminal. An individual whose intent is to get his or her hands on a tangible gain - money - uses the computer as a metaphorical pistol pointed at a bank teller. But where the computer is the object, things are not so clear. These situations, of course, are not limited to theft of the computer itself, but to those things associated with it which have substantial value but which are not tangible and whose legal status is unclear. For example, the information stored in a computer can be of inestimable value to its processor and to others and can be "stolen" without damage to the computer and without "depriving" the owner of its use. This applies to perhaps the most valuable information in a computer - the program - the key to how the machine carries out its data processing. And an even more intangible, yet valuable "thing" that can be taken is computer time. So great is the capacity of a computer and so valuable are its services that use of it even for short periods of time can be of great worth. The degree to which

these intangibles can or should be protected is a significant issue for the law.

This leads to a brief discussion of how computer crime is carried out. A computer has five principal component parts. First there is the input which converts data and instructions from human-readable to machine-readable codes. The central processing unit controls and coordinates the machines and the data based on its operating instructions, or program, also known as software. This is the heart of a cybernetic machine. All other processes are basically mechanical and repetitious, but made significant by the vast memory capacity and great speed of their operation, but software is qualitatively different - it governs how that data is to be processed. Next, the logical and memory units perform calculations, decision-making and storage functions in response to commands from the control unit. Finally, the output unit converts processing results back into human-readable language or symbols. A typical computer system may also use telecommunications facilities in order to link the central unit with terminals or printers located elsewhere.(4)

A computer system is vulnerable to invasion and abuse at virtually every component part. Personnel can alter data at the input stage; operations and systems programmers can manipulate data and software; transmission of data over common carrier lines can be tapped; and both authorized and unauthorized users can interfere with computer operations at terminals. The methods used to perpetrate theft or fraud by computer range from the ingenious to the banal. The following are some examples:

1. Data Diddling

This is described as "the simplest, safest, and most common method used in computer related crime."(5) Anyone who creates, records, transports, encodes, examines, checks or otherwise has access to data that will enter a computer has an opportunity to change that data to his or her

---

(4) Canada, *Changing Times: Banking in the Electronic Age,* Interdepartmental Steering Committee on the Electronic Payments System, Ottawa, 1979, p. 250.

(5) U.S. Department of Justice, Bureau of Justice Statistic, *Computer Crime - Criminal Justice Resource Manual,* Washington, D.C. 1979, p. 9.

advantage before it enters processing. For example, a time clerk who filled out data forms for payroll purposes noticed that overtime claims were entered into the computer by employee number and not name. He accordingly put his number against the claims of other employees who worked overtime frequently, and received extra income over a period of time.(6)

2. **Salami Techniques**

This form of automated crime is so named because it involves stealing small amounts of assets from a large number of sources without noticeably reducing the whole. One form is the "round down" fraud. It involves alteration of the processing of bank interest calculations. Typically, interest calculations are rounded to the nearest cent and distributed among all accounts involved. The perpetrator modifies the program so that the remainder of all accounts rounded down are funnelled to an account over which he or she has control. Supposedly such a technique is virtually undiscoverable since customers would not notice the absence of fractions of a cent and auditors would not delve too deeply into such a program; although the return is not great, this crime would accumulate a tidy profit over time.(7)

3. **Scavenging**

This can be one of the less sophisticated forms of computer crime. It refers to the securing of information that may be left in or around a computer system after it has been used for a job. It can be as simple as searching trash barrels for copies of discarded computer listings or carbon papers from multiple-part forms used in input. In another example, time-sharing computers are involved. Frequently computer tapes are not erased but merely written over by the next user. A person seeking information can secure a tape used by a competitor, enter a small amount of data and read the entire tape back out, scavenging the information from the previous job.(8)

---

(6) *Ibid.*, p. 10. He was apprehended when an auditor noticed his unusually high income on a tax form and investigated further.

(7) *Ibid.*, p. 13-16.

(8) *Ibid.*, p. 23.

The foregoing are just a few of the techniques used to perpetrate a computer-assisted crime. Many can be combatted through improved security and personnel evaluation and clearance methods. When theft or fraud is carried out by use of a computer the victim will usually eventually find out, because tangible property is being affected. But what of the "theft" of software or other information, or of computer services? This can be carried out, often without damage, instantaneously and without the owner's awareness. To prevent unauthorized use, code numbers, passwords and encryption devices are used. But these may be only as reliable as the personnel to whom they are divulged. The close association of various clients and businesses can vitiate these security devices(9) and there are techniques whereby access controls can be overridden by exploiting weaknesses in computer response to unauthorized attempts to breach its security.(10)

THE SIGNIFICANCE OF COMPUTER CRIME

The overall significance of computer crime is difficult to assess. Some contend that the statistics available are not reliable for such incidents because there is a more profound unwillingness to report computer-related crime than any other. One writer(11) has identified four reasons why discovered crimes are not reported or prosecuted:

1) the overall or imagined fear of the loss of public confidence;

2) the difficulty of proving that a crime has been committed;

3) concern about possible liability for lack of prevention of the incident;

---

(9) J.D. Parker, *Crime by Computer,* Scribner's, New York, 1976.

(10) Whiteside (1978), p. 115-126.

(11) S. Sokolik, "Computer Crime - The Need for Deterrent Legislation" (1980), 2 *Computer Law Journal* 353, at 359.

4) the user's belief that public exposure of the incident would be tantamount to an admission of vulnerability, as well as instruction to others on how to commit the crime.

Research has confirmed this unwillingness to publicize such incidents. The manager of a data processing division of a large corporation defrauded his employer by using $61,000 of computer time to operate his own computing business. The company declined to bring charges against him because it had already been a victim of a bigger fraud, which it did not want revealed. Another case involved a public utility company which "handled internally" a situation in which three employees had appropriated the company's computer system in order to trade on the commodities market.(12)

One body of opinion holds that computer abuse, even if widespread, should not be a matter of concern for legislators. According to this view, crime accomplished with the computer as instrument is fully prosecutable under existing substantive law (with perhaps some modification in procedural law, especially in rules of evidence). Other abuse, such as "theft" of information, or of computer time should be left to the civil law or innovation will be stifled.

One critic(13) contends that actual computer-assisted crime is much less prevalent than popularly believed and that a certain mystique has unfortunately attached to the whole area. He points to the celebrated *Rifkin* case in which a computer technician in California managed to have $10 million transferred from a bank computer to a Swiss bank account. The press characterized him as a "computer wizard" who had somehow manipulated the machine in some arcane way, when in fact he had done no more than steal a transfer code and impersonate a bank officer by telephone. His acts were prosecuted under existing penal law.(14) As for other computer crimes, the critic doubts the accuracy of reports of

---

(12) Canada, *Changing Times: Banking in the Electronic Age*, p. 253.

(13) J. Taber, "A Survey of Computer Crime Studies" (1980), 2 *Computer Law Journal* 275.

(14) For a full account see: J. Becker, "Rifkin, A Documentary History" (1980), 2 *Computer Law Journal* 471.

incidents and holds, further, that some alleged "crimes" are, in a practical sense, impossible to commit. He contends, for example, that the "round down" computer fraud (see p. 5) is a myth, both impractical in view of existing banking procedures and logically incapable of bringing in more than miniscule returns.(15)

As for the security of computer systems, it is contended that this should not be an area for the penal sanction, but one in which users and owners should look out for their own interest by improving security and exercising civil remedies. The attachment of criminal consequences to unauthorized use could have serious effects on the computer industry. For example the common recreational and private use of "spare" computer time by programmers, operators and other users is regarded by many as a job perquisite akin to using a company telephone for limited personal calls. By making unauthorized access a crime such activities would be viewed as a theft of private property.(16)

Opponents of this laissez-faire view contend that the role of computer technology is so great and can affect so many people beyond its owners and direct users, that some form of legislative intervention is necessary. In addition, computer time and efficiency are so valuable that existing lax industry standards of security should no longer be tolerated.

THE CANADIAN CONTEXT

The distinction between computer as instrument and computer as object is useful in an analysis of Canadian criminal law respecting computers and the reforms of the 1980s.

Where the computer was used as the instrument of crime, there had been successful prosecutions under various provisions of the *Criminal Code*. A supervisor of accounts with a large company used a computer system to generate cheques payable to a fictitious company he

---

(15) Taber (1980), p. 311-327.

(16) R. Kling, "Computer Abuse and Computer Crime as Organisational Activities" (1980), 2 *Computer Law Journal* 403 at 406.

had created by changing the numbers in invoices of regular customers. The cheques were sent to an accomplice, and the company lost over $100,000. The supervisor was convicted of fraud (section 338 of the Code) and sentenced to imprisonment. In another case, an employee of a stockbroker had permission to trade for his own account. He removed his trading losses from the employer's computer, manipulated balance figures after each day's dealings and doctored ledger books to make them balance also. In this way his losses could not be traced and were periodically written off. Over a period of six months he acquired between $65,000 and $100,000. He was subsequently convicted of theft and received a prison sentence of three years.(17) The major problem in such cases was not so much the application of substantive criminal law to the impugned conduct, as the detection and proof of the activities.(18)

Where the computer was the object of abuse, more serious problems arose because much of the conduct in this area was imperfectly dealt with by the *Criminal Code*, if at all.

A celebrated case took place at the University of Alberta in 1977. The computer system there, a substantial one serving the whole university community, was connected to over 300 terminals on campus, and also to telecommunication facilities. In the summer of 1977 the system was experiencing an unusual number of "crashes" or shutdowns of the system, up to five crashes in a week; more than one crash a week was considered

---

(17) Canada, *Changing Times: Banking in the Electronic Age*, p. 263, 266.

(18) In the case of *R.* v. *McMullen* (1979), 47 C.C.C. (2d) 499, the Ontario Court of Appeal held that in order for a computer printout to be entered as evidence it was necessary to prove the facts of the complete record-keeping process (i.e., input of entries, storage of information, and its retrieval and presentation). However, in *R.* v. *Bell and Bruce* (1982), 65 C.C.C. (2d) 377, the same court later held that computer printouts constituted "records" within the meaning of section 29(2) of the *Canada Evidence Act*, and, therefore, were admissible on the strength of affidavit evidence, a decision eventually affirmed by the Supreme Court of Canada (see *Bruce* v. *The Queen*, [1985] 2 S.C.R. 287). While there is little doubt that today's courts recognize the value of computer-produced evidence, it seems that clear standards of admissibility have yet to be developed; Kenneth L. Chasse, "Business Documents: Admissibility of Computer-Produced Records," *Crown Newsletter*, 1991, p. 27.

unsatisfactory. It was determined that these were not being caused by equipment failure, but by improper programming. It was apparent that some unauthorized person was gaining access to the system, examining areas of batch data, interfering with the input of data, and acquiring other users' confidential passwords. University personnel monitored the system and, employing the computer's ability to identify the origin of its user, apprehended a student at one of the terminals. After an investigation it was determined that the student, Christensen, had been working closely with two others, McLaughlin and Astels. All three were charged with theft of telecommunication service:

> Everyone commits theft who fraudulently, maliciously, or without colour of right...
>
> (b) uses any telecommunication facility or obtains any telecommunication service.(19)

They were also charged with mischief:

> Everyone commits mischief who wilfully...
>
> (c) obstructs, interrupts or interferes with the lawful use enjoyment or operation of property.(20)

At trial, Astels was acquitted on both counts, owing to a reasonable doubt as to whether he had been informed that he was prohibited from using the computer; hence, he could plead "colour of right." Christensen, the student caught "red-handed," was convicted of both charges. The judge found that the computer could be considered a telecommunication facility within the definition in section 287(2):

> ... "telecommunication" means any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system.

The judge based his decision on the fact that the computer system was connected by telephone and coaxial cables to the telephone system and that there could be dial up connection through telephone lines to the central

---

(19) Section 287(1) of the *Criminal Code*.

(20) Section 387(1) of the *Criminal Code*.

processing unit. The "crash" caused by Christensen had interfered with and interrupted the lawful use of university property and accordingly he was also guilty of mischief.(21) McLaughlin was also convicted under section 287. It was found that he had given Christensen programs and information and encouraged him to use the computer. He was thus found to be a party to the offence under section 20 of the Code in that he had aided and abetted the commission of the offence. He was acquitted of the mischief charge, however, because no evidence linked him with the "crash" which his friend had caused. He had aided in the theft but not the consequent mischief.

McLaughlin appealed his conviction on the ground that a computer system was not a "telecommunication facility." The Alberta Court of Appeal allowed the appeal,(22) and this decision was upheld by the Supreme Court of Canada on 18 July 1980. The Court ruled that although the computer system was connected to telephone facilities and was an electronic system, its function was not the transmission and reception of information, the hallmark of telecommunication. Rather, its *raison d'être* was data processing:

> ... the function of the computer is not the channelling of information to outside recipients so as to be susceptible in that respect to unauthorized use. Rather, it is to permit the making of complex calculations, to process and correlate information and to store it and enable it to be retrieved.(23)

Mr. Justice Estey added:

> Had Parliament intended to associate penal consequences with the unauthorized operation of a computer, it no doubt would have done so in a section of the *Criminal Code* or other penal statute in which the term which is now so permanently embedded in our language is employed. The court would not be expected by Parliament to glean from words generally associated with the communications industry an intent to attach penal consequences to the unauthorized operation of a computer.(24)

---

(21) *R.* v. *Christensen et al.* (1978), 26 *Chitty's Law Journal* 348, at 353.

(22) *R.* v. *McLaughlin* (1979), 12 C.R. (3d) 391.

(23) (1980), 18 C.R. (3d) 339, at 345, per Laskin, C.J.C.

(24) *Ibid.*, p. 349.

The decision caused something of a stir in the computer industry. It was interpreted to mean that there was nothing to prevent or deter anyone from making unauthorized use of computer facilities. This was not entirely true. It should be remembered that Christensen was convicted of "mischief," which can be treated as an indictable offence and carry up to a five-year sentence, for the "crash" he had caused. But it was questionable whether a mischief charge would stand for unauthorized access and use without a crash, for section 387 required obstruction and interruption of, or interference with a property owner. Conceivably, a skilled intruder could use a computer without directly contravening those prohibitions.

The *McLaughlin* case was the most detailed Canadian judicial treatment of issues related to the computer as the object of abuse, but there were other significant issues dealing with certain "intangibles" related to computers which existing Canadian criminal law did not clearly address. For example, information or data stored in a computer, particularly software or programs, can be extremely valuable. Such data can be taken in an instant, without damage to computer hardware, or without depriving the owner of the data store therein. Did taking computer data in itself constitute an offence under the *Criminal Code?*

That issue came before the courts in the case of *R.* v. *Stewart.*(25) The accused Stewart, a self-employed consultant, was charged with the offences of counselling theft and fraud when he attempted to obtain from a hotel security officer a copy of a computerized list of the names and addresses of the hotel's employees. The employee list was sought by the accused's client who wanted to organize the employees into a union.

Acquitted at trial, the accused was convicted on appeal. In a two-to-one decision, the Ontario Court of Appeal held that confidential information, such as a list of employees, came within the meaning of the terms "property" and "anything" as those terms are used in connection with

---

(25) *R.* v. *Stewart* (1982), 68 C.C.C. (2d) 305 (Ont. High Court); (1983), 35 C.R. (3d) 105 (Ont. Court of Appeal); (1988), 50 D.L.R. (4th) 1 (S.C.C.).

the offences of theft and fraud at sections 283 and 338 (now sections 322 and 380) of the *Criminal Code*.[26] Accordingly, the accused was guilty of both offences, although he could be convicted of only one since both counts flowed out of the same delict.

In his reasons for judgment, Mr. Justice Houlden held, on the one hand, that the accused was guilty of counselling a section 283(1)(d) theft, since had he been successful in obtaining the list, he would have dealt with the information in such a manner that it could not be returned to its owner, the hotel, in the same condition as it had been at the time of the taking, i.e., the information would have lost its "confidential" character. On the other hand, he found that for the offence of fraud it was sufficient to prove a risk of prejudice to the economic interests of the hotel; it was not necessary to show actual economic loss by reason of the fraud. Since the hotel could have sold its list of employees to promotional groups and therefore, could have profited from such a venture, the unauthorized taking of the list by the accused would have caused a risk of prejudice to the hotel's economic interests.

In a concurring judgment, Mr. Justice Cory added that although information *per se* was not property, there was a "right of property" in confidential information which came within the meaning of the term "property" at section 283(1). Citing copyright as an example of an enforceable proprietary interest, he held that the accused was guilty of counselling theft since he had sought to obtain from the security officer

---

(26) The relevant provisions of the *Criminal Code* stated:
283(1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate, with intent,
(a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it.
.....
(b) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.
338(1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security [is guilty of an offence].

an unauthorized copy of the computerized list, thereby infringing the hotel's property interest in the list.

In a dissenting judgment, Mr. Justice Lacourcière would have sustained the acquittal on the ground that the term "anything" at section 283 had to be defined and qualified within the context of property, and that confidential information simply did not fit within that context. In his view, it was up to Parliament and not the courts to broaden the criminal definition of the property concept if the needs of Canadian society required it. Moreover, he felt that the mere loss to the hotel of the "confidentiality" of its information was not sufficiently prejudicial to its economic interests as to constitute a criminal fraud.

Mr. Stewart appealed his conviction for theft to the Supreme Court of Canada. If the majority judgment of the Ontario Court of Appeal had been sustained on appeal, it might have had far-reaching social implications, for what was at stake was not simply the attempted theft of a computerized list of employees, but more importantly, the broader issue of theft of information at large, regardless of its storage medium. Should information be treated as property, whether "confidential," "copyrightable" or otherwise? Was the criminal law an appropriate vehicle to sanction its misappropriation?

In a reversal of the Ontario Court of Appeal decision, the Supreme Court of Canada held that confidential information does not come within the meaning of the word "anything" in section 282 (now section 322) of the *Criminal Code*. To be the subject of theft, "anything" must be property in the sense that it has to belong to someone and it must be capable of being taken or converted in a manner that results in a deprivation of the victim. The Court found that confidential information does not constitute "property" for the purposes of the criminal law respecting theft and cannot *per se* be the subject of a taking, or of a conversion when the owner is not deprived of it.

Writing for a unanimous court, Mr. Justice Lamer also held that the nature of the information taken would not support a conviction for fraud, since the complainant had not been deprived of any money or economic advantage.

PARLIAMENTARY ACTION

A. The Sub-Committee on Computer Crime

On 9 February 1983, the subject-matter of Bill C-667, an Act to amend the *Criminal Code* and the *Canada Evidence Act* in respect of Computer Crime, was referred to the Standing Committee on Justice and Legal Affairs. The bill, introduced by the Hon. Perrin Beatty apparently in response to the legislative vacuum created by the *McLaughlin* case (the *Stewart* case had not come before the courts), sought, among other things, to (1) amend the definition of "property" in the *Criminal Code* to include computer software products, (2) create the offence of "computer theft" (the fraudulent diversion of a computer program to one's own or another person's use), and (3) expand the mischief provisions to encompass the unauthorized destruction, alteration or damage of computer programs.

In response to the order of reference, a Sub-committee on Computer Crime was established on 10 March 1983 with representation from the three parties. In the course of its hearings, the Sub-committee heard considerable evidence from a wide range of witnesses with expertise in such diverse fields as computer technology, security and management, computer law, the law of intellectual property, law enforcement, banking, privacy rights and consumer protection.(27) The Report of the Sub-committee on Computer Crime was tabled in the House of Commons on 29 June 1983.(28)

In its report, the Sub-committee agreed that the existing law was inadequate to deal with a number of computer-related abuses and concluded that, even though the incidence of computer crime in Canada was not known, there was a sufficient potential for serious harm to justify the enactment of criminal sanctions. However, the Sub-committee was not persuaded that the best way to proceed was expressly to include computer software products in the definition of "property." In its view, to treat computerized data as property might lead to more problems than it would

---

(27) *Minutes of Proceedings and Evidence* of the Sub-committee on Computer Crime of the Standing Committee on Justice and Legal Affairs, 32nd Parliament, 1st Session, 1980-81-82-83, Issues No. 1 to 17.

(28) *Ibid.*, Issue No. 18.

resolve, given the special status afforded information in our socio-legal system. Moreover, the Sub-committee felt that it would be inconsistent to proscribe the misappropriation of computerized data without, however, proscribing the misappropriation of information stored in other media.

For these reasons, the Sub-committee opposed the suggestion that the theft provisions of the *Criminal Code* be expanded expressly to cover the misappropriation of computerized information. Instead, it recommended the creation of two new offences prohibiting certain computer-related misconduct.

1) the unauthorized access (without colour of right) to a computer system; and

2) the unauthorized destruction and alteration (without colour of right) of computerized data.

The Sub-committee expressed the view that the enactment of criminal sanctions was but one way of discouraging computer-related abuses. Stressing the desirability of prevention over punishment, it recommended that the computer industry and institutional users adopt appropriate security measures, and that computer ethics be made an integral part of computer training. Moreover, finding that the misappropriation of computerized data could not be dealt with in isolation from the broader issue of information misappropriation, the Sub-committee concluded that a comprehensive approach to the problem had to be taken. In its view, legislative action was also needed to provide enhanced civil remedies to guard against information misappropriation and, therefore, recommended that other relevant laws (copyright, patent, trade secrecy, etc...) be examined and modified where necessary.

B. Legislative Response

1. *Criminal Law Amendment Act, 1985*

Criminal Code amendments dealing with computer crime came into effect on 4 December 1985. The various legislative provisions are substantially in keeping with the recommendations of the Sub-committee on

Computer Crime. On the one hand, unauthorized use of a computer is proscribed by section 342.1:

> (1) Everyone who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system.
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.
>
> (2) In this section,
>
> "computer program" means data representing instructions or statements that, when executed in a computer system, cause the computer system to perform a function;
>
> "computer service" includes data processing and the storage or retrieval of data;
>
> "computer system" means a device that, or a group of interconnected or related devices one or more of which,
>
> (a) contains computer programs or other data, and
> (b) pursuant to computer programs,
> (i) performs logic and control, and
> (ii) may perform any other function;
>
> "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

On the other hand, section 430 proscribes mischief in relation to data:

> (1.1) Everyone commits mischief who wilfully
>
> (a) destroys or alters data;
> (b) renders data meaningless, useless or ineffective;
> (c) obstructs, interrupts or interferes with the lawful use of data; or

> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
>
> (5) Everyone who commits mischief in relation to data
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
> (b) is guilty of an offence punishable on summary conviction.
>
> (5.1) Everyone who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
> (b) is guilty of an offence punishable on summary conviction.
>
> (8) In this section, "data" has the same meaning as in section 342.1.

These measures avoid the problems that would have ensued from treating computerized data as property. By proscribing actions relative to, rather than focusing on ownership of, computerized data, the types of misconduct encountered in the *McLaughlin* and *Stewart* cases are effectively dealt with, without, however, venturing into the more dangerous zone of information ownership.

2. *An Act to Amend the Copyright Act*, S.C. 1988, c. 15

Also in keeping with the recommendations of the Sub-committee, were additional steps taken to address the issue of unauthorized appropriation of software materials. As a result of 1988 amendments to the *Copyright Act*, "computer program" is now defined and included in the definition of "literary works" protected under the Act. In addition to the civil remedies available for infringement of copyright, the Act makes it an offence punishable on summary conviction or indictment. Additional 1988 amendments increased the penalties for that offence to a maximum of one million dollars and/or five years' imprisonment, for conviction on indictment.